-14-

REMARKS

The Examiner has rejected Claims 1-12, 16-27, and 31-42 under 35 U.S.C. 103(a) as being unpatentable over Asai et al. (U.S. Patent No. 6,760,765) in view of Hailpern et al. (U.S. Patent No. 6,275,937) in view of Grantages, Jr. et al. (U.S. Patent No. 6,510,464). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to the independent claims. Specifically, applicant has amended the independent claims to at least substantially include the subject matter of former dependent Claims 13, 28, and 43.

With respect to the independent claims, the Examiner has relied on the following excerpts from the Grantages reference to make a prior art showing of applicant's claimed technique "wherein, upon receipt of an access request, the processing logic is arranged to determine from the access request predetermined attributes, and to send those predetermined attributes to the file storage device to enable the file storage device to perform a validation check, the processing logic only allowing the access request to proceed if the file storage device confirms that the client device is allowed to access the file identified by the ... access request" (see this or similar, but not necessarily identical language in the independent claims).
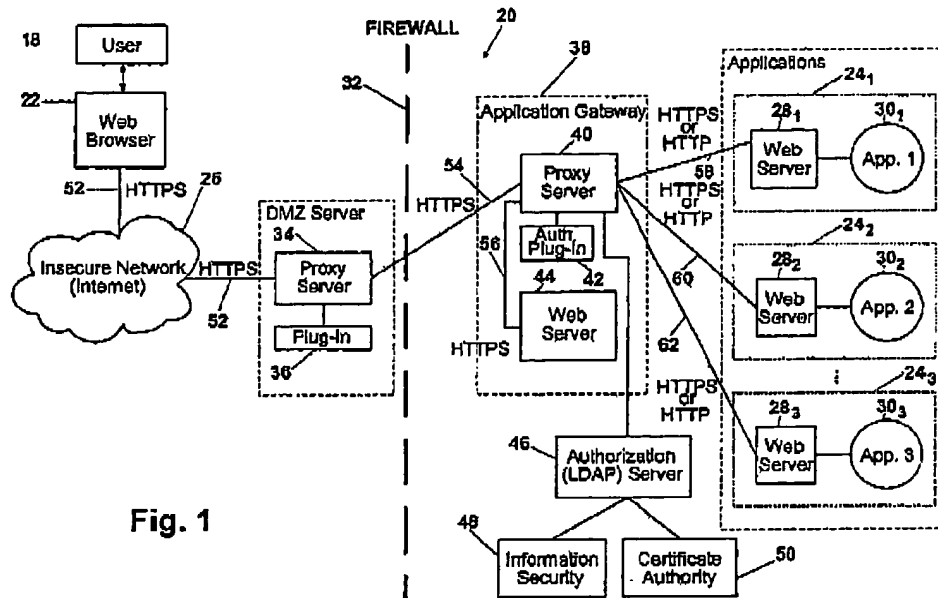
-15-

Fig. 1

(Grantages, Fig. 1, items 34 and 40, not cited)

"Computer system 20 includes a firewall system 32, a **proxy server 34 with a plug-in 36, an application gateway 38 comprising a gateway proxy server 40 with a plug-in 42 and a gateway web server 44, and an authorization server 46.**" (Grantages, Col. 4, lines 15-19 - emphasis added)

"The **user-selected X.509 digital certificate is then sent to proxy server 34. At this point, a first level authentication is conducted, outside the firewall, by proxy server 34** (e.g., checks to see whether the X.509 certificate has been issued by a predetermined preapproved certificate authority). If authenticated at this level, **proxy server 34 then sends the information contained in the client's digital certificate through firewall system 32 to gateway 38 to be authenticated at a second,** more substantive level. The second level authentication involves examining the particulars of the X.509 digital certificate using the data stored on authorization server 46." (Grantages, Col. 4, lines 43-55 - emphasis added)

Applicant respectfully asserts that the above excerpts relied upon by the Examiner teach the use of proxy servers for authentication. In particular, Grantages discloses a technique where the "... first level authentication is conducted, outside the firewall, by proxy server ..." Grantages continues to disclose that the "proxy server 34 then sends the information contained in the client's digital certificate through firewall system <u>32 to gateway 38 to be authenticated</u>" (emphasis added) where the "... application gateway 38

-16-

compris[es] a gateway proxy server 40." Figure 1 of Grantages clears shows the gateway proxy server 40 communicating with the authorization server 46 in order to "us[e] the data stored on authorization server 46." However, using the proxy servers to perform authentication simply fails to meet a technique "... to send those predetermined attributes to the file storage device to enable the file storage device to perform a validation check ..." (emphasis added), as claimed by applicant.

In addition, the Examiner has relied on the following excerpts from the Grantages reference to make a prior art showing of applicant's claimed technique "wherein a user cache is utilized for storing the predetermined attributes" (see this or similar, but not necessarily identical language in the independent claims).

```
"Before proceeding to a detailed description of computer system
20, a general overview of the operation established by the
invention will be set forth, as viewed by user 18 of client
computer 22. Initially, user 18 of client computer 22 enters the
destination URL into a web browser portion of client computer 22.
The web browser then issues an HTTP request across insecure
network 26, which is routed to proxy server 34. The user 18 may
then be presented with a "popup" message that a secure network
connection is about to be established. The message may also ask
which X.509 digital certificate user 18 wishes to use for
authentication. The user-selected X.509 digital certificate is
then sent to proxy server 34. At this point, a first level
authentication is conducted, outside the firewall, by proxy
server 34 (e.g., checks to see whether the X.509 certificate has
been issued by a predetermined preapproved certificate
authority). If authenticated at this level, proxy server 34 then
sends the information contained in the client's digital
certificate through firewall system 32 to gateway 38 to be
authenticated at a second, more substantive level. The second
level authentication involves examining the particulars of the
X.509 digital certificate using the data stored on authorization
server 46. If user 18 is authorized to access multiple
applications, the next item after the "popup" message to be
displayed to user 18 is an "options page", presenting the
multiple choices. Once a particular application is selected, the
next item to be displayed for user 18 is a welcome page of the
selected application. Secure, authenticated remote access is
complete. In accordance with the present invention, computer
system 20 provides an efficient mechanism for routing the remote
user 18 of client computer 22 to the selected application being
served by one of the destination servers." (Grantages, Col. 4,
lines 33-65 - emphasis added)
```

Applicant respectfully asserts that the above excerpt from Grantages relied upon

-17-

by the Examiner discloses a technique of "... examining the particulars of the X.509 digital certificate using the data stored on authorization server..." (emphasis added). However, the rejection of applicant's claimed "user cache" is moot due to amendments made to the independent claims clarifying such claimed element. Specifically, applicant has amended the independent claims to require a technique "wherein the proxy device comprises a user cache utilized for storing the predetermined attributes" (emphasis added). Thus, the excerpt from Grantages clearly fails to teach applicant's claimed technique, particularly as amended.

In addition to the above remarks, the Examiner has rejected Claims 14, 15, 29, 30, 44, and 45 using the same excerpts and arguments found in the Office Action mailed on 09/12/2005. These dependent claims, however, were previously incorporated by applicant into the independent claims in the Amendment D dated 12/08/2005, and thus no longer exist. To this end, the previously submitted (and unconsidered) remarks are reiterated below for full consideration by the Examiner.

In particular, the Examiner relies on the excerpt from Webb below to meet applicant's claimed technique "wherein, upon receipt of an access request, the processing logic is arranged to determine from the access request predetermined attributes, and to send those predetermined attributes to the file storage device to enable the file storage device to perform a validation check, the processing logic only allowing the access request to proceed if the file storage device confirms that the client device is allowed to access the file identified by the file access request; wherein a user cache is utilized for storing the predetermined attributes" (see this or similar, but not necessarily identical language in each of the independent claims)

```
"[0048] A Web page is served to the user's client that identifies
each device on the private network for which the user has access
rights (Block 240). According to alternative embodiments of the
present invention, a secure cookie containing the user's log-in
information and having a specified life span (e.g., 15 minutes
after the last access) may be returned to the user's client with
the served Web page (Block 245). The cookie may allow the user to
access the Web server of any device that the user is authorized
to access, but only for a specific time period. Each time the
```

-18-

```
user accesses a device on the private network, the user's client
sends the cookie to the gateway and the gateway determines
whether the user is authorized to access the particular device.
Upon expiration of the specified time period, the user would be
required to log-in with the gateway. It is understood that
embodiments of the present invention are not limited to the use
of cookies. Alternatively, user log-in and/or session information
may be encoded within a URL."
```

It appears that the Examiner has not taken into consideration the full weight of applicant's claims. Specifically, the foregoing excerpt discloses that the gateway receives a cookie from a client and the gateway determines whether the user is authorized to access a particular device. Further, it appears that the Examiner assumes the following in Table 1.

<u>Table 1</u>

gateway   = claimed "proxy"

cookie   = claimed "attributes"

particular device   = claimed "file storage device"

Assuming this, Webb still fails to meet applicant's claimed technique "wherein, upon receipt of an access request, the processing logic is arranged to determine from the access request predetermined attributes, and <u>to send those predetermined attributes to the file storage device to enable the file storage device to perform a validation check</u>, the processing logic <u>only allowing the access request to proceed if the file storage device confirms that the client device is allowed to access the file identified by the file access request</u>" (emphasis added). Only applicant teaches that the validation is performed by the <u>file storage</u> which, in turn, controls the proxy device in the manner claimed. Still yet, applicant also disagrees that the mere disclosure of a data structure such as a cookie meets applicant's claimed <u>user cache</u> utilized for storing the predetermined attributes, as claimed.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the

-19-

reference or to combine reference teachings.   Second, there must be a reasonable
expectation of success. Finally, the prior art reference (or references when combined)
must teach or suggest all the claim limitations. The teaching or suggestion to make the
claimed combination and the reasonable expectation of success must both be found in the
prior art and not based on applicant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d
1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie*
case of obviousness has not been met, since the prior art references, when combined, fail
to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite
such paramount deficiencies and in the spirit of expediting the prosecution of the present
application, applicant has amended the independent claims to further distinguish
applicant's claim language from the above reference by incorporating the subject matter
of Claims 13, 28, and 43, as follows:

"wherein the proxy device comprises a user cache-utilized for storing the

predetermined attributes" (see this or similar, but not necessarily identical

language in the independent claims).

With respect to the subject matter of former Claims 13, 28, and 43 (now at least
substantially incorporated into the independent claims), the Examiner has rejected the
same under U.S.C. 103(a) as being unpatentable over Asai in view of Hailpern in view of
Sathyanarayan et al. (U.S. Patent No. 6,304,904). Specifically, the Examiner has relied
on the following excerpts from the Sathyanarayan reference to make a prior art showing
of applicant's claimed feature.

> "Transcode manager 22 selects an appropriate transcode service
> provider 24 based, for example, on the content type of the data
> stream. In this context, the term content type encompasses a
> datatype, an HTTP MIME (Multipurpose Internet Mail Extensions)
> type, a content format, and so on. The selected transcode service
> provider 24 uses a separate thread to read the incoming data
> stream, transcode it (for example, scan for predetermined content
> and delete it if found), and place it within the entry of server-
> side cache memory 30." (Sathyanarayan, Col. 5, lines 23-32)

-20-

"Transcoding server 34 may be configured to provide a wide
variety of transcoding services to network client 12 and/or
network devices, such as content servers, with which network
client 12 communicates. In this context, the term "transcode"
refers to virtually any type of addition, deletion or
modification of data transmitted to or from network client 12 by
or through transcoding server 34. In addition to the collection
of statistics as set forth herein, examples of such transcoding
services include data compression, image scaling, and dynamic
removal of predetermined content. In the context of the present
invention, the collection of statistics may be the only
transcoding service provided to a particular client device, or
may be only one of a variety of services." (Sathyanarayan, Col.
3, lines 7-20 – emphasis added).

Applicant respectfully asserts that the above excerpt from Sathyanarayan relied
upon by the Examiner teaches caching incoming data into a server side cache memory.
Specifically, the excerpt discloses to "read the incoming data stream, transcode it (for
example, scan for predetermined content and delete it if found), and place it within the
entry of server-side cache memory 30" (emphasis added). However, the technique of
deleting predetermined content before placing into the server side cache memory, as set
forth in the above excerpt, fails to meet a technique "wherein the file cache is arranged
only to store files which have been determined not to be considered as malware" (emphasis
added), as claimed by applicant.

Applicant further notes that the prior art is also deficient with respect to the
dependent claims. For example, with respect to Claims 6, 21, and 36, the Examiner has
relied on the following excerpts from the Asai reference to make a prior art showing of
applicant's claimed technique "wherein the proxy device interface is arranged to receive a
ready signal from each proxy device in said plurality indicating whether that proxy device is
ready to receive an access request, the load balancing routine being arranged to refer to said
ready signals when determining to which proxy device to direct a particular access request."

"Next, a fail-safe operation is now described. In the fail-safe
operation, even when any one of the cache servers in the cluster
server apparatus becomes unable to carry out data distribution to
the terminals due to a failure that occurred in the any one of
the cache servers, another cache server takes over for the failed
cache server so as to continue data distribution.

-21-

As stated above, the cache server 10.sub.x distributes the
streaming data to the terminal 4.sub.y, while notifying the cache
server 10.sub.x+1 or 10.sub.x-1 of the information corresponding
to the distributed streaming data at regular intervals (step
S110, S126, S132). On the other hand, the distribution-disabled
detection units 13.sub.x+1 and 13.sub.x-1 of the cache servers
10.sub.x+1 and 10.sub.x-1, respectively, monitor the information
received at regular intervals from the cache server 10.sub.x.

Now consider the case in which the cache server 10.sub.x has a
failure and becomes unable to carry out data distribution to the
terminal 4.sub.y. It is assumed herein that the cache servers
10.sub.x and 10.sub.x+1 manage certain streaming data in common.

In the above case, when the distribution information, which is
supposed to arrive at regular intervals from the cache server
10.sub.x, does not arrive, the distribution-disabled detection
unit 13.sub.x+1 of the cache server 10.sub.x+1 detects a
distribution-disabled (occurrence of failure) state of the cache
server 10.sub.x. When the distribution-disabled detection unit
13.sub.x+1 detects the distribution-disabled state, the data
distribution unit 12.sub.x+1 reads streaming data that succeeds
the streaming data most recently distributed by the cache server
10.sub.x from the streaming data storage unit 15.sub.x+1 based on
the distribution information previously received from the cache
server 10.sub.x (before the failure occurs), and then distributes
the read streaming data that succeeds the streaming data most
recently distributed before the failure of the cache server
10.sub.x to the terminal 4.sub.y. This distribution and reading
operation is carried out within a predetermined time period so as
not to interrupt the streaming data. The predetermined time
period means a time period during which the streaming data most
recently distributed is completely played back in the terminal
4.sub.y." (Asai, Col. 17, lines 10-47 - emphasis added)

Applicant respectfully asserts that the excerpt(s) from Asai relied upon by the
Examiner teaches the use of "another cache server [that] takes over for the failed cache
server so as to continue data distribution" (emphasis added) and that "the cache server
10.sub.x distributes the streaming data to the terminal 4.sub.y, while notifying the cache
server 10.sub.x+1 or 10.sub.x-1 of the information corresponding to the distributed
streaming data at regular intervals" (emphasis added). However, "the cache server ...
notifying the cache server ... at regular intervals" (emphasis added), as set forth in the
above excerpt, fails to even suggest a technique of "a ready signal ... indicating ... that
proxy device is ready to receive an access request" (emphasis added), as claimed. More
particularly, the excerpt from Asai above fails to disclose a technique "wherein the proxy
device interface is arranged to receive a ready signal from each proxy device in said
plurality indicating whether that proxy device is ready to receive an access request, the load

-22-

balancing routine being arranged to refer to said ready signals when determining to which proxy device to direct a particular access request" (emphasis added), as claimed by applicant.

In addition, with respect to Claims 7, 22, and 37, the Examiner has relied on the following excerpts from the Asai reference to make a prior art showing of applicant's claimed technique "wherein each device in the computer network is assigned an identifier, and the load balancing device is assigned the same identifier as is assigned to the file storage device, the client interface being connectable to a communication infrastructure of the computer network to enable communication between the load balancing device and said client devices, whilst the plurality of proxy devices are connectable to the proxy device interface and the file storage device is connectable to each proxy device, such that the file storage device is only accessible by said client devices via said load balancing device and one of said proxy devices."

FIG. 1
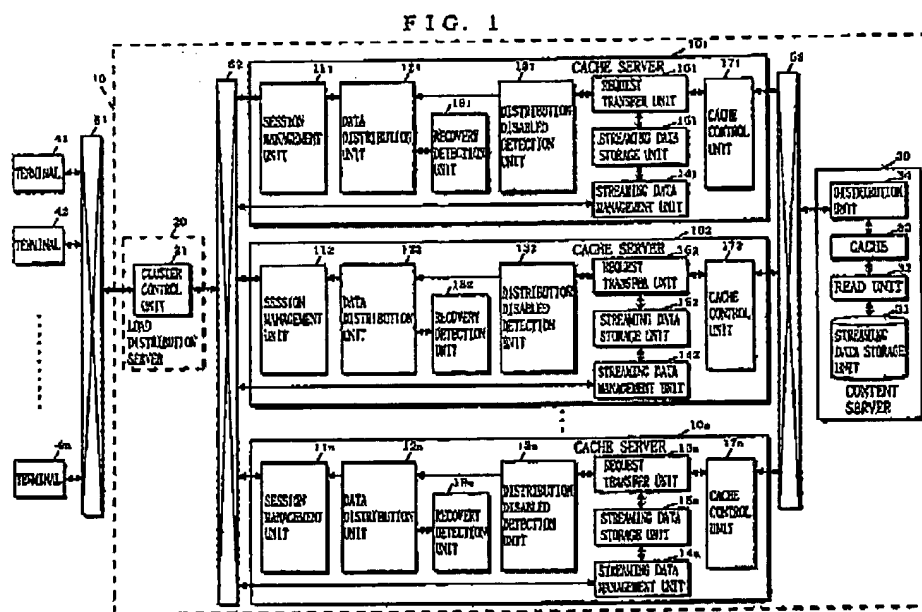
(Asai, Figure 1)

Applicant respectfully asserts that the figure from Asai relied upon by the

-23-

Examiner fails to disclose applicant's claimed technique where the file storage device and load balancing device are assigned the same identifier, as claimed. In reference to the Examiner's argument that "an inherent feature of a server-side proxy farm is that the gateway has the address on the internet which is used for the content server, thereby ensuring that the load balancer is not bypassed to get to the content server," applicant respectfully notes that the following emphasized claim language is simply not found in the above excerpt: "wherein each device in the computer network is assigned an identifier, and the load balancing device is assigned the same identifier as is assigned to the file storage device" (emphasis added), as claimed by applicant.

It appears that the Examiner has relied on an inherency argument regarding the above emphasized claim limitations. In view of the arguments made hereinabove, any such inherency argument has been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested. (See MPEP 2112). Further, applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art reference fails to teach or suggest all the claim limitations. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 46-51 below, which are added for full consideration:

"wherein the access requests are buffered when the proxy device is busy and unable to process the access requests utilizing the load balancing device" (see Claim 46);

"wherein the access requests are buffered when the proxy device is busy and unable to process the access requests utilizing the proxy device" (see Claim 47);

-24-

"wherein the load balancing device maintains an additional cache including details about the access requests utilizing the proxy devices" (see Claim 48);

"wherein the additional cache is utilized to allocate subsequent access requests for a particular file to one of the proxy devices that handled a previous access request for the particular file" (see Claim 49);

"wherein the malware scanning is not performed when the file has already been scanned" (see Claim 50); and

"wherein the predetermined attributes in the user cache are re-used by the proxy device during the processing of the access request" (see Claim 51).

Again, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The

-25-

Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P476).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100